METHOD AND COMMUNICATIONS DEVICE FOR SECURE GROUP COMMUNICATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This is the first application filed for the present invention.

MICROFICHE APPENDIX

[0002] Not Applicable.

TECHNICAL FIELD

[0003] This invention relates in general to secure communications in a highly dynamic environment and, in particular to a method and communications device for enabling secure group communication in a highly dynamic environment

BACKGROUND OF THE INVENTION

[0004] The development of Internet enabled group-oriented applications such as audio and video conferencing, stock quotes, and pay-per-view have become very popular. However, achieving secure and convenient group collaboration in a highly dynamic environment is a significant challenge for several reasons.

[0005] First, preventing a message exchanged among group members from being received or intercepted by non-members is a core problem of group communication. It requires authentication and secrecy. With respect to authentication, there are two types in common use — message authentication and source authentication. Message authentication only guarantees that a message was sent by

a certified group member, without telling who sent the message. Source authentication identifies who sent the message and is therefore more desirable. Data secrecy requires not only data communication secrecy, but also secure forward secrecy, so that when a member leaves or is removed from a group, that member can no longer receive messages exchanged within the group. Likewise, data secrecy requires backward secrecy, so that when a new member joins a group, that member can receive an inspect only those messages exchanged within the group after the new member has joined.

[0006] Moreover, in some circumstances group members frequently leave and/or new members frequently join the group. It is therefore imperative that a solution be provided for supporting highly dynamic communications groups.

[0007] Scalability is another important criterion for evaluating group communication solutions, and a good solution must not rely on the architecture of the underlying network.

[0008] Group-oriented communication research is presently one of the fastest growing areas in the field of networking. There are two trends in current solutions for secure group communication. One is non-collaborative group key management, as taught, for example in RFC 2627 entitled Key Management for Multicast: Issues and Architectures, Wallner et al.(1999); Secure Group Communications Using Key Graphs, Wong et al. (1998); and United States Patent No. 6,240,188, which issued May 20, 2001 to Dandeti et al., entitled Distributed Group Key Management Scheme for Many-to-Many Communications. The

other is collaborative group key agreement, as taught, for example in an article entitled New Multiparty Authentication Services and Key Agreement Protocols; Ateniese et al., IEEE Journal of Selected Areas of Communications, Vol. 18, No. 4, April 2000; and Diffie-Hellman Key Distribution Extended to Group Communication, Steiner et al. third ACM Conference on Computer and Communications Security. Each of these solutions is based on establishing a group key shared by all members, and re-keying when group members change. Consequently, performance is degraded in large groups with frequent membership changes.

[0009] The representative non-collaborative group key management solutions are the tree-based solutions. Typical collaborative key agreement solutions are based on Diffie-Hellman key exchanges. Tree-based solutions rely on a trusted central controller for key distribution and management. Although they work well in relatively static groups, they are not appropriate in certain circumstances. For example, in ad hoc wireless networks where a fixed central control is non-existent or difficult to identify. In addition, such systems are vulnerable because there is a signal point of failure (or attack).

[0010] The peer-to-peer collaborative group key agreement solutions have certain desirable features, such as distributed key management, key authentication and key confirmation. However, they are too complex and computationally intensive for practical use.

[0011] There therefore exists a need for a method and communications device for secure group communication that is reliable and practical to use.

SUMMARY OF THE INVENTION

[0012] It therefore is an object of the invention to provide a method and communications device for secure group communication that is easy to implement and practical to use.

[0013] The invention therefore provides a communications device for secure communications in a highly dynamic environment between members of a predefined communications group that includes a plurality of group members. The communications device comprises an orthogonal code module for maintaining an orthogonal code table by reciprocally exchanging an orthogonal code with a communications device operated by each new member that joins the group, and deleting from the table the orthogonal code associated with the communications device of any group member that leaves the group; an encryption module for encrypting a message to be sent to one or more of the group members using the orthogonal code associated with respective communications devices operated by the group members to which the message is to be sent; and a decryption module for decrypting a message sent from a communications device operated by any of the other group members.

[0014] The invention also provides method of providing secure communications in a highly dynamic environment between members of a predefined communications group that includes a plurality of group members. The method comprises maintaining an orthogonal code table for each group member by reciprocally exchanging an orthogonal code with each new member that joins the group, and deleting from the table the orthogonal code associated with any group member that leaves the group; encrypting a message

to be sent to one or more of the group members using the orthogonal code associated with respective group members to which the message is to be sent; and decrypting a message sent from a communications device operated by any of the other group members.

[0015] The invention therefore supports source authentication because for any recipient of a message, there is a specific orthogonal code associated with a sender of the message, and the recipient can only decrypt a message sent by the sender using the specific orthogonal code.

[0016] The invention also provides not only data communication secrecy but also forward access and backward access secrecy. Since the orthogonal codes used by the respective group members are pseudo-random and independent, if a member leaves a group and the related orthogonal codes are deleted, the former member cannot decrypt future communications among the group members within a reasonable period of time. Similarly, if a new member joins, new orthogonal codes will be assigned to the new member, but with those newly assigned orthogonal codes, the new member cannot deduce the orthogonal codes of others within a reasonable period of time, or decrypt the communications conducted prior to the time that the member joined the group.

[0017] The invention also adapts well to highly dynamic situations because there is no group key formation and re-keying problem involved. Consequently, there is little communications overhead that results from a membership change.

[0018] The invention requires no assumptions about the underlying network, and the message length is not linearly related to the number of message recipients. The invention therefore demonstrates excellent scalability.

[0019] Finally, the invention can be used even though the communications devices of the respective group members have a wide range of different capabilities.

[0020] Moreover, the invention is very flexible because each member makes an independent decision about whether to exchange orthogonal codes with other group members. Therefore, the invention achieves secure communication within arbitrary subgroups, as well as providing both one-way and two-way secure communications within a group at the same time.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] Further features and advantages of the present invention will become apparent from the following detailed description, taken in combination with the appended drawings, in which:

[0022] FIG. 1 illustrates an exemplary structure of an orthogonal code table stored by each group member;

[0023] FIG. 2 illustrates an exemplary preparation process for orthogonal code exchange;

[0024] FIG. 3 illustrates the format of an orthogonal codes exchange message;

[0025] FIG. 4 illustrates an orthogonal code exchange between group members;

[0026] FIG. 5 illustrates a procedure for amalgamating a number of messages for a number of group members;

[0027] FIG. 6 is a flow diagram that illustrates a message encryption process in accordance with the invention;

[0028] FIG. 7 is a flow diagram that illustrates message amalgamation in accordance with the invention;

[0029] FIG. 8 illustrates a procedure for extracting a message from a received amalgamated message; and

[0030] FIG. 9 illustrates a process required when a member leaves the group or a new member joins the group.

[0031] It will be noted that throughout the appended drawings, like features are identified by like reference numerals.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0032] FIG. 1 illustrates an exemplary structure for an orthogonal code table 10 in accordance with the invention stored on a communications device belonging to each group member. As shown, there is a group member list 12 that stores the identifiers of all other group members, a corresponding encryption orthogonal code list 14, and a corresponding decryption orthogonal code list 16. The encryption orthogonal code list 14 stores the orthogonal codes assigned by the owner of the table to the members of the group member list 12. Correspondingly, the decryption orthogonal code list 16 stores the orthogonal codes assigned by the members of the group member list to the owner of the secure code table 10.

[0033] FIG. 2 illustrates the process of preparing orthogonal codes for exchange with the group members. As shown, the preparation process includes the following steps:

a) A member queries a credentials database 18 for any encryption means or encryption keys 20 belonging to an orthogonal code recipient. The encryption key 20 can be a public key or a symmetric key depending on the data stored in the credentials database 18 by the orthogonal code recipient.

b) The member encrypts an orthogonal code 22 that it assigns to the recipient using the encryption means or encryption key 20 to obtain an encrypted orthogonal code 24.

c) The encrypted orthogonal code 24 is encapsulated with an secure header 26.

d) After all other group member orthogonal codes are encrypted, the member concatenates all the encapsulated encrypted orthogonal codes into a code message 28, adds the sender ID 30 and the recipient list 32 to form an orthogonal codes exchange message 34.

[0034] FIG. 3 shows the format of an orthogonal codes exchange message 34, which includes the sender ID 30, the recipient list 32, and a concatenate encrypted code message 28. Each part of the concatenated encrypted code message 28 includes an secure header 26 and an encrypted orthogonal code 24. The secure header 26 contains a key identifier and a bit indicating the encryption means

employed for orthogonal code exchange with the corresponding recipient.

[0035] FIG. 4 illustrates an orthogonal codes exchange among group members. As shown, each member broadcasts an orthogonal codes exchange message 34 to all other members. When a member receives the orthogonal codes exchange message 34, the group member's communications device locates its copy of the encrypted orthogonal code using the key identifier in the header 26 and uses the appropriate decryption means to decrypt the orthogonal code.

[0036] FIG. 4 further shows that after a recipient receives the orthogonal code exchange messages 34 from one or more group members, the communications device broadcasts an amalgamated orthogonal code confirmation to all group members from which a code message 34 was received. The procedure for generating an amalgamated orthogonal code confirmation is the same as the procedure of amalgamating any other message which will be explained below in detail. In accordance with the invention, broadcast is preferably used for message distribution to save communication overhead.

[0037] FIG. 5 illustrates the procedure for amalgamating messages for two or more group members. As shown, a communications device 40 owned by a group member encrypts a message 42 for a recipient by encrypting it (44) using the encryption orthogonal code 14 obtained from the orthogonal code table 10. The sender encrypts two or more messages for two or more recipients in parallel, and the communications device 40 outputs the encrypted messages to an adder 46, which outputs an amalgamated secure

message 50. The adder 46 may be implemented in parallel to improve the performance. In addition, the messages 42a-42n for the different recipients may be the same or different, so that arbitrary group members can be selected as a subgroup to receive an identical message.

[0038] FIG. 6 is a flow diagram of an exemplary message encryption process. The process starts at step 100 in which the encryption orthogonal code is transformed to bipolar form ('1' transformed to '+1'; '0' transformed to '-1'). The procedure proceeds to step 102 in which the message to be sent is transformed to binary (0,1) form. At step 104, it is determined whether the end of the message has been reached, which indicates that message encryption is complete. If so, then the resulting encrypted message is output to the adder 106. If not, the process advances to step 108 and a next bit of the binary message is inspected. The content of the bit determines one of the three actions:

- if the bit is a "1" (step 110), the bit is replaced with the encryption orthogonal code, and the process returns to step 104;

- if the bit is a "0" (step 114), the bit is replaced with a negative of the encryption orthogonal code, and the process returns to step 104.

[0039] FIG. 7 is a flow diagram of message amalgamation. After the messages for all recipients are encrypted and output to the adder (step 106), those encrypted messages are added together bit by bit at step 160, and an amalgamated secure message is generated at step 162.

[0040] FIG. 8 illustrates an exemplary process for extracting a message from a received amalgamated message. When a communications device 40 operated by a group member receives an amalgamated message 162, the communications device 40 accesses its orthogonal code table 10 to retrieve the corresponding decryption orthogonal code 16 associated with the sender ID 12 of the sender. The communications device 10 extracts the message 170 intended for the recipient by computing a normalized inner product of the amalgamated secure message 162 and decryption orthogonal code 16. Due to the secure property of the codes, only the group member who has the corresponding orthogonal code can retrieve the appropriate part of the message, as will be explained below in more detail. At the same time, any recipient who does not possess the sender's orthogonal codes 14 cannot decode the message or any other part of a message except that part intended for them.

[0041] FIG. 9 illustrates the process when a member leaves or a new member joins a communications group. If a new member wants to join the group, as shown in FIG. 9(a), the process begins at step 200 where the new member sends a join request to all the members that the member wishes to securely communicate with. At step 202, each member decides independently if they will accept communications from the new member. If not, the member returns a refuse confirmation at step 204. Otherwise, the recipient exchanges orthogonal codes with the new member using the process as illustrated in FIG. 2, omitting the concatenation process. Likewise, the new member sends orthogonal codes to the accepting members using the process illustrated in FIG. 2.

[0042] When a member leaves (step 210) the group, as shown in FIG. 9(b), all remaining group members update (step 212) their orthogonal code table 10 by deleting the row used to store codes for the departing member.

Code Generation

[0043] There are several algorithms that may be used for orthogonal code generation, such as an secure variable spreading factor (OVSF) Code Generator, a Hadamard Code Generator, or a Walsh code generator, for example.

Code Example

[0044] In the following, an orthogonal code generated by the OVSF code generator is used as an example for illustrating the encryption and decryption algorithms.

[0045] In this example, there are four group members. **S** is a sender and **A**, **B**, **C** are recipients. The orthogonal codes for **A**, **B** and **C** are [1, 1, -1, -1], [1, -1, 1, -1], and [1, -1, -1, 1] respectively. Those skilled in the art will understand that these example codes are used for simplicity of illustration only, and are not intended to represent an actual implementation. In general, the code length will be considerably longer than show here by way of illustration.

[0046] In a first example, **S** sends a binary message "101" to **A**, **B** and **C**.

Message preparation:

Encryption:

For **A**, the encrypted message is: [1,1,-1,-1,-1, -1,1,1,1,1,-1,-1] (1)

For **B**, the encrypted message is: [1,-1,1,-1,-1, 1,-1,1,1,-1,1,-1] (2)

For C, the encrypted message is: [1,-1,-1,1, -1,1,1,-1,1,-1,-1,1] (3)

Amalgamation:

Add (1), (2), and (3)

Resulting message is: [3,-1,-1,-1,-3,1,1,1,3, -1,-1,-1] (4)

Decryption:

When **A** gets the message (4), the internal product is computed and formalized:

$(4)\cdot[1,1,-1,-1]*1/4=[(3-1+1+1),(-3+1-1-1),(3-1+1+1)]*1/4=[1,-1,1]$

i.e. the message recovered is "101"

Similarly, **B** and **C** recover the message using the same process.

[0047] As a further example, suppose **S** sends "10" to **A**, "01" to **B**, "11" to **C**.

Message preparation:

Encryption:

For **A**, the encrypted message is: [1,1,-1,-1,-1, -1,1,1] (1)

For **B**, the encrypted message is: [-1,1,-1,1,1, -1,1,-1] (2)

For **C**, the encrypted message is: [1,-1,-1,1,1,-1, -1,1] (3)

Amalgamation:

Add (1), (2), and (3)

Resulting message is: [1,1,-3,1,1,-3,1,1] (4)

Decryption:

When **A** receives the message (4), the internal product is computed and formalized:

$(4)\cdot[1,1,-1,-1]*1/4=[(1+1+3-1),(1-3-1-1)]*1/4=[1,-1]$

The message recovered is "10".

When **B** receives the message (4) the internal product is computed and formalized:

$$(4)\cdot[1,-1,1,-1]*1/4=[(1-1-3-1),(1+3+1-1)]*1/4=[-1,1]$$

The message recovered is "01".

When **C** receives the message (4), the internal product is computed and formalized:

$$(4)\cdot[1,-1,-1,1]*1/4=[(1-1+3+1),(1+3-1+1)]*1/4=[1,1]$$

The message recovered is "11".

[0048] As will be understood from the above example by those skilled in the art, more compact messages can be achieved using the methods in accordance with the invention if a user assigns more than one encryption code to each other group member with which the user communicates.

[0049] The invention therefore provides a method and a communications device 40 for enabling secure communications among members of a group in a highly dynamic environment, such as a wireless fidelity or an Internet environment where others apart from group members may receive or intercept messages exchanged between group members.

[0050] The embodiment(s) of the invention described above is(are) intended to be exemplary only. The scope of the invention is therefore intended to be limited solely by the scope of the appended claims.